

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 May 2002 (10.05.2002)

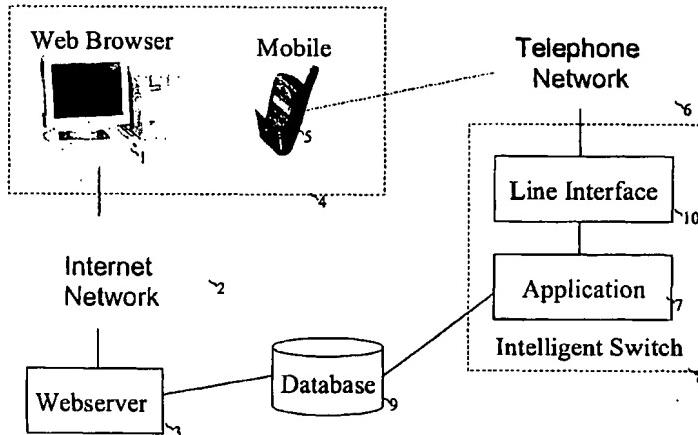
PCT

(10) International Publication Number
WO 02/37240 A2

- (51) International Patent Classification⁷: G06F 1/00
- (21) International Application Number: PCT/GB01/04835
- (22) International Filing Date:
1 November 2001 (01.11.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
00309635.1 1 November 2000 (01.11.2000) EP
- (71) Applicant (*for all designated States except US*): BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).
- (72) Inventors; and
- (75) Inventors/Applicants (*for US only*): THOMPSON, Stephen, Michael [GB/GB]; 7 Borrett Place, Martlesham, Woodbridge, Suffolk IP12 4TU (GB). MCCARTNEY,
- (52) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: COMPUTER SYSTEM



WO 02/37240 A2

(57) Abstract: When a user of a web browser (1) attempts to access a web server (3) through an Internet network (2) then the web server (3) transmits a security code and telephone number to the web browser (1) for display. A number to be called is selected from a plurality of network nodes as stored in a database (9), which is accessible to the security means of the web server (3) and an application (7) in an intelligent switch (8) attached to, for example the PSTN. The web server (3) monitors the database (9) for a CLI and PIN entered against the selected network node number. The intelligent switch application (7), on receiving calls through a line interface (10) from, for example, a mobile telephone (5) associated with a particular user will store the CLI and PIN entered on receipt. Provided that the CLI is valid and the PIN entered is correct, then the access attempt is permitted. Alternatively, when an access attempt is made from a web browser (1) to the web server (3) a PIN may be transmitted to the mobile phone (5) associated with the alleged user and the input from the web browser (1) monitored for correct return of the PIN within a predetermined period.



Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Computer System

The present invention relates to a computer system and more particularly to security for such systems which are accessible by multiple users.

- 5 Over a comparatively short period of time electronic communication has allowed unprecedented access to information stored in computer databases, and has allowed processing of information to facilitate so-called e-commerce. Information, communication and entertainment can be obtained from many sources under control of an individual using a keyboard or some other form of direct or indirect
10 communication with file servers which may control the distribution of or access to stored data and/or programs. Such access using so-called connectionless networks, such as the world wide web or Internet can cause security problems where confidential information is stored and/or where a pecuniary advantage might be obtained, for example by obtaining goods and services in a fraudulent manner.
- 15 It is well known to control access across a network by using personal user name in combination with a password or PIN but it has been found that such password arrangements can be broken by determined effort and/or by effecting multiple accesses using a computer program to obtain fraudulent access to systems.

It is also known to restrict access to a computer system to particular known
20 terminals or from particular known telephone lines (identified for example by terminal address or telephone line identity). Such systems reduce the opportunity for fraudulent access, particularly if used in combination with a user/password arrangement. However, such systems are inherently inflexible if a user requires mobility – that is the ability to access a system from a number of different places
25 and/or by way of a connectionless network which may not provide a constant IP address for a particular terminal.

In published PCT Application no WO/95/19593 there is disclosed a method of securing access by transmitting transformation codes through a paging network. Thus when a user identification is input to a host computer system a random code is
30 generated which is transformed using a user-specific algorithm. The generated code is then transmitted to a special pager terminal which uses an in-built algorithm to transform the transmitted code which code is then input by the user for comparison with the transformed code at the host computer. Necessarily the user requires to

carry an additional non-standard item (the adapted pager) in order to access the computer system.

According to the present invention there is provided a computer system accessible by way of a network, the system including means responsive to an access attempt by way of a first communications route to transmit a security characterisation code to an assumed user using a return path associated with said first communications route and to monitor a second communications route for input of the characterisation code, the system denying access if the security characterisation code is not correctly received on the second communications route.

10 Preferably the security characterisation code is retrieved from secure server means which is responsive to an access request to provide a random security code for transmission to the presumed user.

In an alternative mode of operation, the security characterisation code is transmitted to a known communications destination associated with the presumed user, for example a cellular telephone or other addressable communications node, the computer system monitoring the access for input of the correct security code and denying access if the code is not entered within a pre-determined period after transmission.

15 In a further enhancement, the security characterisation code is transmitted for display to the user and a communications node is monitored for entry of the characterisation code from a known origination node.

The known origination may be determined by use of caller identity so that only callers from specific associated instruments may access the system.

20 In a further refinement the displayed code is accompanied by one of a selectable plurality of network nodes to which the return call is to be transmitted, the secure server monitoring the network nodes for a call to be placed to the selected one of the plurality and accompanied by the correct characterisation code and an acceptable caller identification.

25 In one operational embodiment there is provided a computer system accessible by way of a network, the system including means responsive to an access attempt by a user to communicate with secure server means to obtain from said secure server means an access code and PIN, the system transmitting the code and PIN to said user, said secure server means being arranged to receive incoming calls

from users on a plurality of nodes determined by a respective plurality of access codes and including means responsive to an access to determine from transmitted signals the identity of a calling terminal associated with said access and to compare said identity with a list of permitted identities, to receive from said calling terminals 5 signals characterising a PIN and to compare the received PIN with a PIN supplied to a computer system in response to a request therefrom and to supply to said computer system an indication of validity of the access attempt.

A computer system in accordance with the invention will now be described by way of example only with reference to the accompanying drawings of which:-

10 Figure 1 is a block schematic diagram of a computer system including a secure server in accordance with the invention;

Figure 2a and 2b show signal interchanges between the web browser and web server of Figure 1;

15 Figure 3 shows inter-operability between the mobile telephone of Figure 1 and the intelligent switch; and

Figures 4 to 11 show screen displays at various stages of the intercommunication used by the computer system.

Referring first to Figure 1, a web browser 1 typically a personal computer or laptop computer or other device capable of communicating by way of an Internet 20 network 2 with web servers 3 (only one of which is shown) is associated with a particular customer as indicated by the dotted line 4. While the web browser apparatus 1 might be permanently associated with the user 4, it may not necessarily be so and access to the web server 3 may be available from any other point of presence of the Internet network 2.

25 Specifically associated with the user 4, there may be a telephone 5, for example a cellular telephone using the GSM or other network. It is not essential for the associated instrument 5 to be a mobile telephone it could be for example a fixed line telephone or another unit capable of receiving messages by way of an addressable communications path. It is also possible that the secondary 30 communications device represented by the instrument 5 is in fact another terminal connected to a node of the Internet network at a known addressable Internet node or having a specific mail box identity for example.

For the purpose of the present description, the apparatus within box 4 is assumed to be specifically associated with the consumer and, will be assumed to allow communication with the consumer by two distinct routes.

- In outline, when a user of the web browser 1 effects a communication with
- 5 a web server 3, either by direct dialling of the web server through a fixed line communications network, for example a telephone network such as the public switched telephone network (PSTN) or through the Internet network 2 to an ISP point of presence then the web server 3, having received information which purports to identify a known user 4, seeks to identify the user 4 by a known secondary route.
- 10 Thus in one example, the web server 3 recovers by way of an application 7, for example, running in association with an intelligent switch 8 of the network and stored in a database 9 a random security code or personal identification number (PIN) together with one of a number of potential network node telephone numbers terminating on the line interface 10 of the intelligent switch 8. The currently selected
- 15 telephone number and PIN is now displayed at the terminal 1 currently in use by the alleged authorised user 4.

- The application 7 now monitors the line interface 10 awaiting an incoming telephony call to any of the numbers with which the application 7 is associated. On receipt of a call the system compares the identification (CLI) of the calling unit 5 and
- 20 uses the CLI for comparison with a list of acceptable identities for the calling unit 5. Assuming the identity corresponds with an acceptable user identity and that the call is received on the correct destination telephone number and further that the entered PIN corresponds with the displayed pin, then the application 7 may cause the web server 3 to accept the access by way of the Internet 2. The checking of the CLI
- 25 against the identity of the alleged user may of course be carried out in the web server 3 rather than in the application 7, the identity being either that of a mobile cellular unit as identified by the cellular communications operator or a PSTN-based CLI.

- As previously mentioned, an alternative is for the characterisation code to be received by way of an alternative terminal attached to the network 2 and having a
- 30 known network address or network identity.

In a first alternative method of operation, when the web server 3 detects an access from an alleged known user 4 (for example identified by a typical user name and password) it may cause a call to be made to a destination communications node

associated with the alleged user 4. This call may now deliver to the alleged user by way of the terminal 5 a randomly generated security code. If the terminal 5 is a mobile phone, then the security code may be voiced to the user as indeed would be necessary if a voice communication to an associated land line were to be made.

- 5 Alternatively, the security code may be transmitted in a short message using the SMS system associated with GSM telephony. Such data messages may also be transmitted to, for example, an ADSL terminal or could be transmitted to a known destination address, for example a mailbox associated with the user in an electronic system.

10 Once again, in this case, the user will be required to enter the security code by way of the keyboard of the web browser 1 for transmission to the web server which may now carry out a comparison between the security code transmitted to the terminal 5 and that received from the terminal 1.

It will be appreciated that in a further alternative scenario the information
15 transmitted by voice or data communication with the terminal 5 might be required to be returned by way of the communication device 5 and the telephone network 6 to the line interface 10 thence to the application 7. It will also be realised that the access from the web browser 1 could be authenticated in a series of steps including receiving a user name and password from the web browser 1 communicating to
20 another terminal associated with the identified user security characterisations, for example PINs and/or selected ones of a plurality of acceptable dial-in telephone numbers and requiring return of the information by way of a further terminal device associated with the identified user.

A specific service will now be described by reference to the remaining
25 Figures so that the specific functionality of one system in accordance with the invention will be recognised. However, while the following specific description relates to a communication from the web browser in the first instance to the web server 3 and requires that a displayed code be transmitted using a mobile phone, for example, 5 the other scenarios outlined above are simple variations of implementation
30 of the invention and are readily implemented once the underlying principle of the invention is understood from the following description.

Referring now to Figure 1 and Figure 2, when a customer 4 using a web browser 1 accesses the web server 3, as indicated at step 21 of Figure 2, the web

server makes an application for a dial-in line number and generates a PIN at steps 22 and 23. Within database 9 the web server sets a marker of line state active in regard to the telephone line to be called in response to the display on the web browser 1 of Figure 1. At step 25 the initial response to the access attempt is now made. This is referred to as a partial response since at this stage the system does not allow access or display of the information requested. This results in the display indicated as step 261, the display being as shown in Figure 4. Thus referring additionally to Figure 4, the display gives an indication of the line to be called, shown here at 01473 663 380, and provides a PIN as generated at step 3 of Figure 2. Contemporaneously, a timer is set in the web server at step 262 awaiting the input from the telephone instrument 5 associated with the anticipated user of the web browser. Now referring additionally to Figure 3 and assuming that the user of the web browser 1 is making a call through the cellular network using the instrument 5, then at step 31 the caller dials in the number displayed as a result of the access by the web server at step 22 and the display at step 261. In the intelligent switch 8 of Figure 1 when a call is received on the line interface 10, the intelligent switch applies to the database 9 for the line status at step 32 this being the line state as set at step 24.

At step 33 a comparison is made of the line state recovered from the web server 3, such that if the line status is not set to active then the current call is an invalid attempt on the selected telephone number. If this is the case that the line status is not active, then the intelligent switch 8 forces termination of the call at step 34, which results in the GSM call terminating as indicated at step 34A.

If, however, the line status is active at step 33, then at step 36 the intelligent switch stores the CLI of the instrument 5 against the line called and sets the line status to done. This may be achieved without answering the call itself if only the CLI and a destination telephone number are to be used as confirmation of the access to the web server 3 from the web browser 1. Thus, after setting the line status to done at step 37, at step 38 the call is again ended by a termination message from the intelligent switch through the GSM network. The returned response to the GSM telephone 5 may be selected from a number of options including transmitting number unobtainable and/or number busy, such that in the case of an unauthorised access attempt the caller does not necessarily have an indication of success in the dial-in attempt.

In the case of a PIN entry requirement in addition to correct CLI, then the intelligent switch application 7 will answer the call and return a call answer to the calling line 5 and will forward a request at step 310 for the PIN displayed in Figure 4 to be entered from the keyboard of the calling instrument. This may be displayed as 5 indicated at 311 as a text message to the phone 5 or may be voiced, for example using text (or data) to speech conversion arrangements (not shown).

As indicated at step 312, the caller now enters the PIN which is collected in the intelligent switch at step 313 and is then stored against the called line. The call will now be terminated by the intelligent switch sending a termination indication to 10 the GSM network and the intelligent switch will return at step 317 to the initial point 30 waiting for calls on one of the lines through the line interface 10.

Referring back to Figure 2, the information stored against the line identity is compared in the web server at step 262 and the web server compares the information stored against the line with that previously transmitted, together with a 15 comparison of the CLI of the GSM phone 5 to determine whether the access attempt has been properly authenticated. Thus, if the call in through the intelligent switch is shown in the database 9 as having no CLI or an incorrect CLI compared to that expected by the web server, then, as shown at Figure 5, a login authentication failure is transmitted to the web browser which will indicate the reason for failure as an 20 invalid CLI. Alternatively, if the call was correctly received from a valid CLI but the PIN entered was not that displayed in Figure 4, then as indicated in Figure 6, failure due to invalid PIN entry will be transmitted. In a further mode, if the line status is not changed to done within the predefined period then the login will fail and a dial-in number expired message will be transmitted at Figure 7.

25 Alternatively, if all of the required features have been received through the intelligent switch from a valid and authenticated calling line, then login authentication is sent as shown Figure 8 and browsing of the secure material or confirmation of the secure transaction may now be made. Thus the final status is sent at step 27 for display on the web browser 1 and if there is no further requirement for the stored PIN, as 30 indicated at step 28, the line state in the database 9 is set to free and if the login attempt was unsuccessful the end response shown in Figure 9 rejecting the attempted access will be transmitted. Assuming that the status of the access attempt was OK then the secure page may be recovered by the user, possibly in

response to further authorisation codes for the required access as indicated at step 211.

If the credentials supplied to the web server from the web browser are not valid, as indicated at step 212, then a reject page at step 212a may be transmitted 5 rejecting the access attempt, for example using the display of Figure 9. If the display request or transaction authentication is rejected, then the session between the web browser 1 and the web server 3 may be rejected and terminated.

If the credentials supplied at 211 are OK and all other certifications appear to be correct, then the web server may build the secure page and transmit it to the web 10 browser 1 for display in known manner, the page content being indicated by the query mark (Figure 10). Prior to transmitting this response however, a check on the entered PIN in the database 9 may be carried out at 214 following which the line status of the identified called line on the line interface 10 may be set to free as previously indicated. Once the response has been sent, the authentication details 15 may be destroyed within the server so that any further attempt to access the secure page will require revalidation through the system. A full response and display may now be sent as indicated at step 216 for display as shown at step 217. A further optional security feature may include ensuring that the displayed page self-destructs after a pre-determined period of time so that information does not remain displayed 20 on an unattended screen for example at the web browser 1. Thus, after the display of the secure data as indicated in Figure 10, automatic logout as shown at Figure 11 may occur. Any further attempt to access information will require the authentication process to be repeated.

It will of course be realised that a single authentication session may give 25 access to a number of secure pages and the question as to whether only a single page access or multiple page accesses are permitted will be determined by the web server content.

As noted above, the system is simply modified to enable alternative authentication to be used. Thus, when a login request is received from an alleged 30 user 4, then instead of expecting a call to a known line selected from a number of valid lines in the database 9, the web server 3 may cause the application 7 in the intelligent switch to effect a call to the instrument 5 and to transmit thereto the required PIN. The data input from the web browser 1 may then be used to check

against a PIN stored against the line to which information was transmitted. Failure to enter the PIN within a pre-determined period will result in the session being terminated.

Since the dial-in line to be used and/or the PIN are randomly generated on an
5 access by access basis, then repeated attempts to break the coding by making
multiple access attempts and entering random PINs is unlikely to succeed.

Although as hereinbefore described, the system communicates between an intelligent switch and the web server using the database 9, it will be appreciated that other means of communication between the switch and server may be used
10 including, but not limited to, shared file space in the web server area for example.

CLAIMS

1. A computer system accessible by way of a network, the system including means responsive to an access attempt by way of a first communications route to
5 transmit a security characterisation code to an assumed user using a return path associated with said first communications route and to monitor a second communications route for input of the characterisation code, the system denying access if the security characterisation code is not correctly received on the second communications route.

10

2. A computer system as claimed in claim 1, in which the characterisation code is retrieved from secure server means.

3. A computer system as claimed in claim 2, in which the secure server means
15 is responsive to an access request to provide a random security code for transmission to a presumed user.

4. A computer system as claimed in any one of claims 1, 2 or 3, having an alternative mode of operation in which the security characterisation code is
20 transmitted to a known communications destination associated with the presumed user.

5. A computer system as claimed in claim 4, in which the security characterisation code is transmitted using a data transmission and display facility.

25

6. A computer system as claimed in claim 1, in which the system causes display of the security characterisation code on a web browser display terminal together with the identity of a randomly selected one of a plurality of telecommunications nodes, the system monitoring a telecommunications line node
30 having a corresponding identity for re-entry of the characterisation code transmitted.

7. A computer system as claimed in claim 5 or claim 6, in which a calling line identity is used to confirm the origin of an incoming call to the system.

8. A computer system as claimed in any preceding claim in which the characterisation code is associated with a decay period after which the code is not valid.
- 5 9. A method of preventing unauthorised access or unauthorised transactions through a first communications route in which on determining an access attempt through the first route a characterisation code is transmitted through an associated path of the first communications route, the characterisation code being transmitted through the first communications route for return by way of a known second
- 10 communications route for comparison with the transmitted characterisation code.
10. A method of preventing unauthorised access or unauthorised transactions as claimed in claim 9 in which a selected one of a plurality of node identities is transmitted together with the first characterisation code, the transmitted node
- 15 identity identifying the second communications route.
11. A method of preventing unauthorised access or unauthorised transactions as claimed in claim 9 or claim 10 in which in addition to comparing the returned code with the transmitted code an identity code associated with a device used for
- 20 communicating with the second communications route is compared with stored identities which identify authorised transmitting devices.

1/8

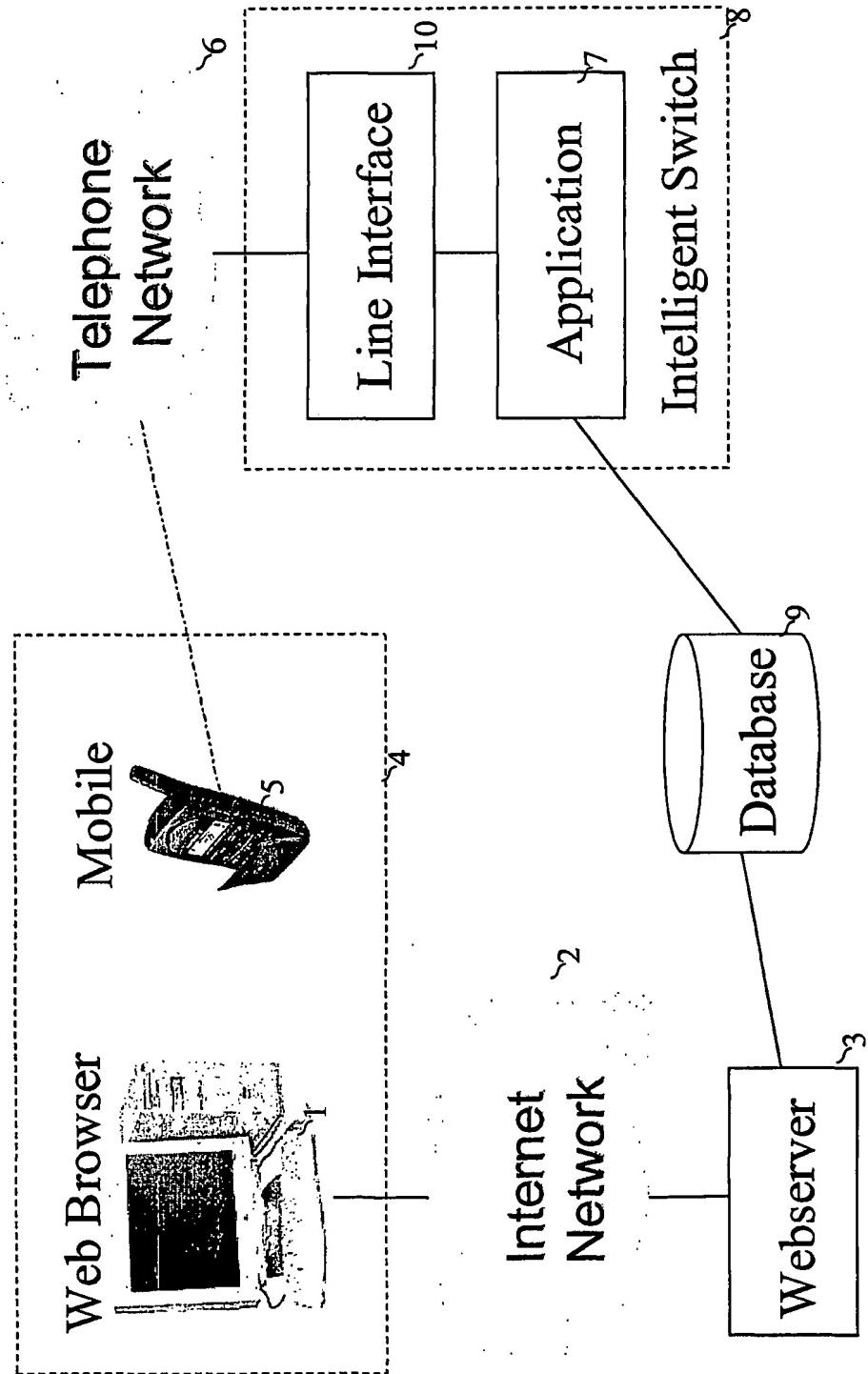


Fig 1

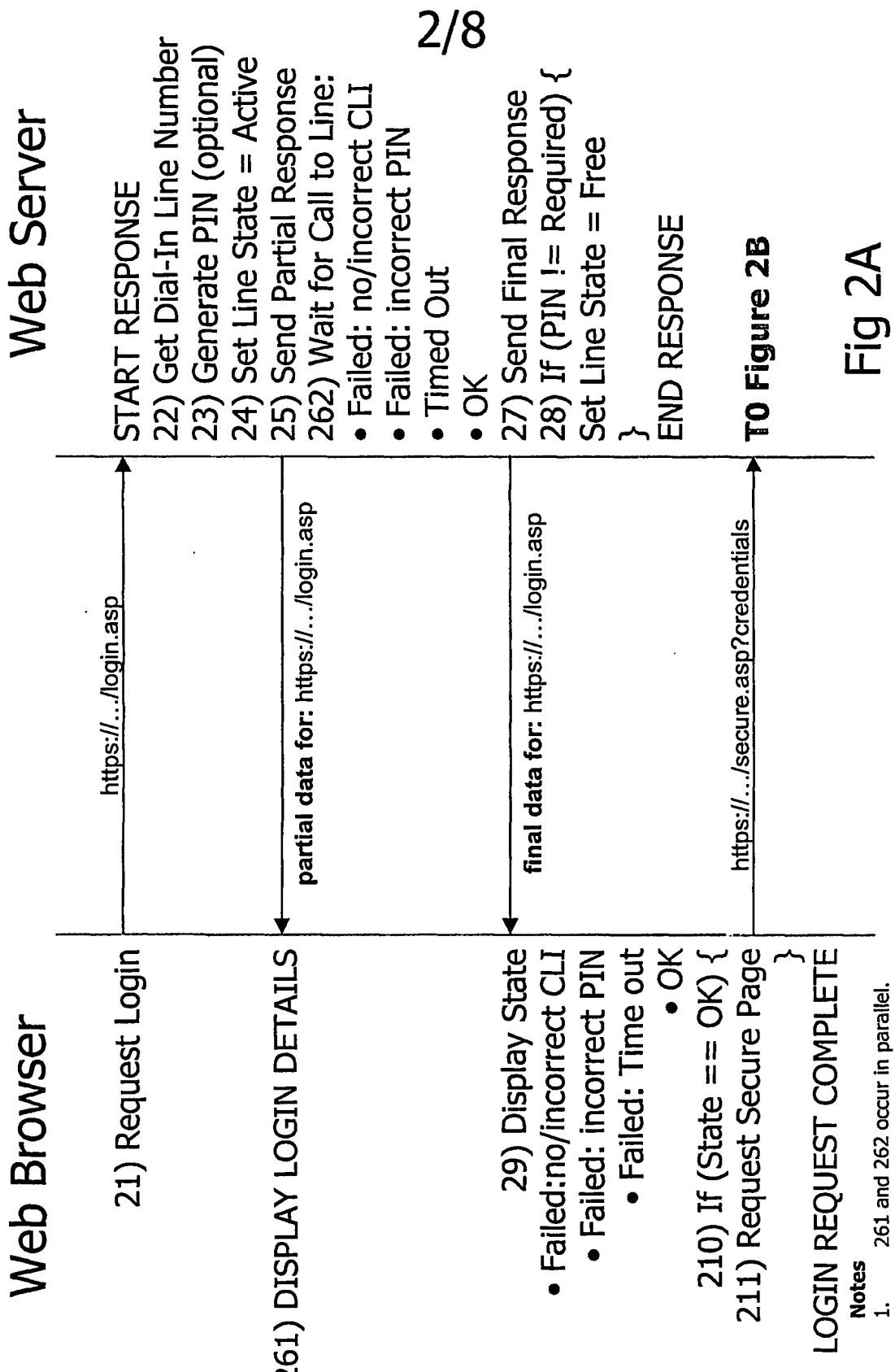


Fig 2A

T0 Figure 2B

Web Server

From Fig 2A

```
START RESPONSE
212) If (Credentials != OK) {
    212a) Serve Reject Page
} Else {
    212b) Build/Serve Secure Page
}
214) If (PIN == Required) or
    Set Line State = Free
}
215) Destroy Credentials
216) Send Response
END RESPONSE
```

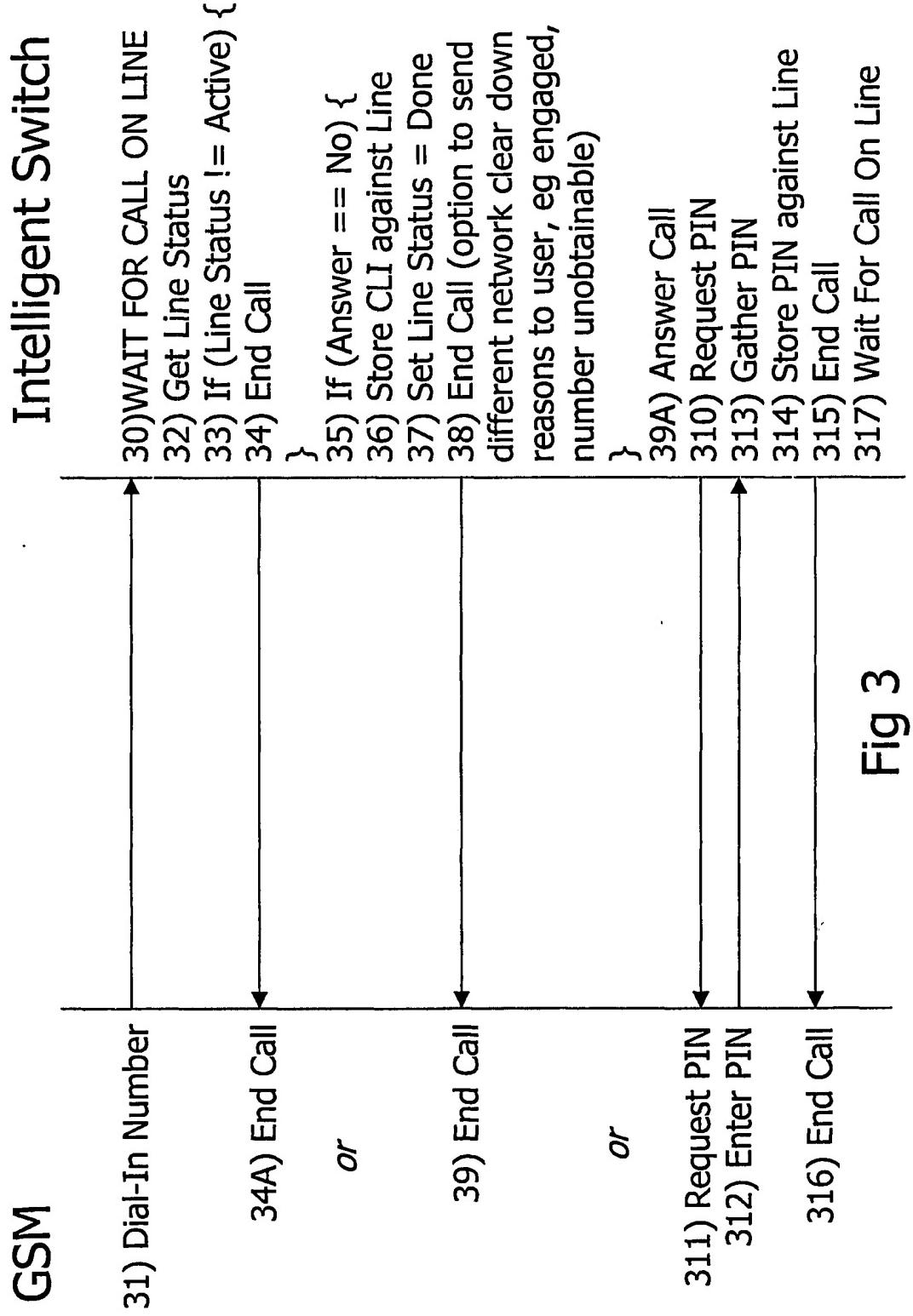
213) Display Reject Page
redirect to https://.../reject.asp

or

217) Display Secure Page
218) Secure Page self destruct
(optional)
SECURE SESSION ENDS

Fig 2B

4/8

**Fig 3**

5/8

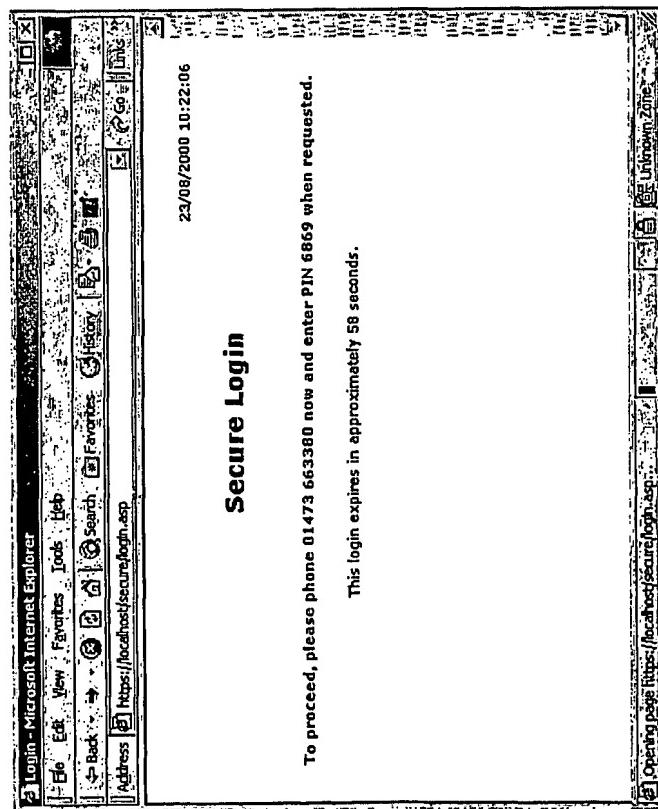
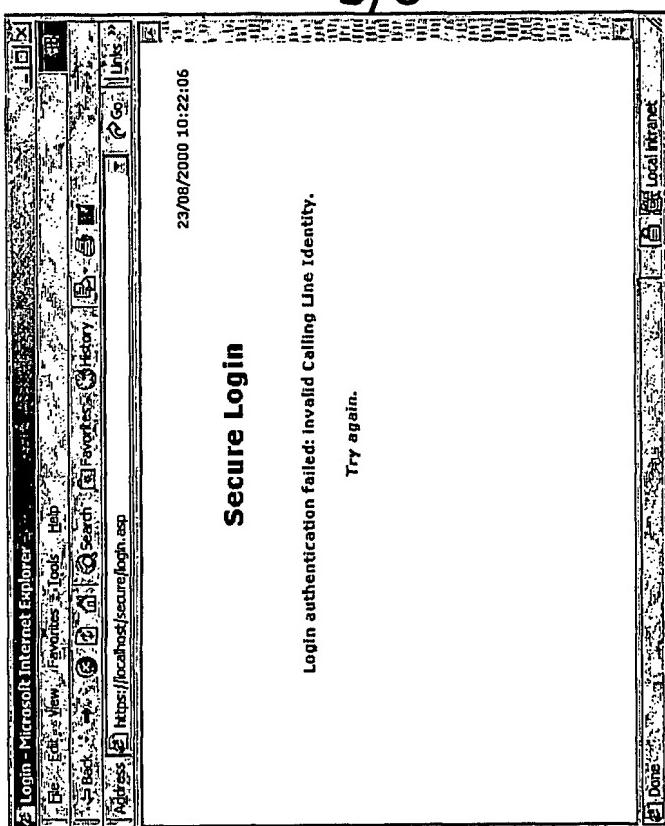


Fig 5

Fig 4

6/8

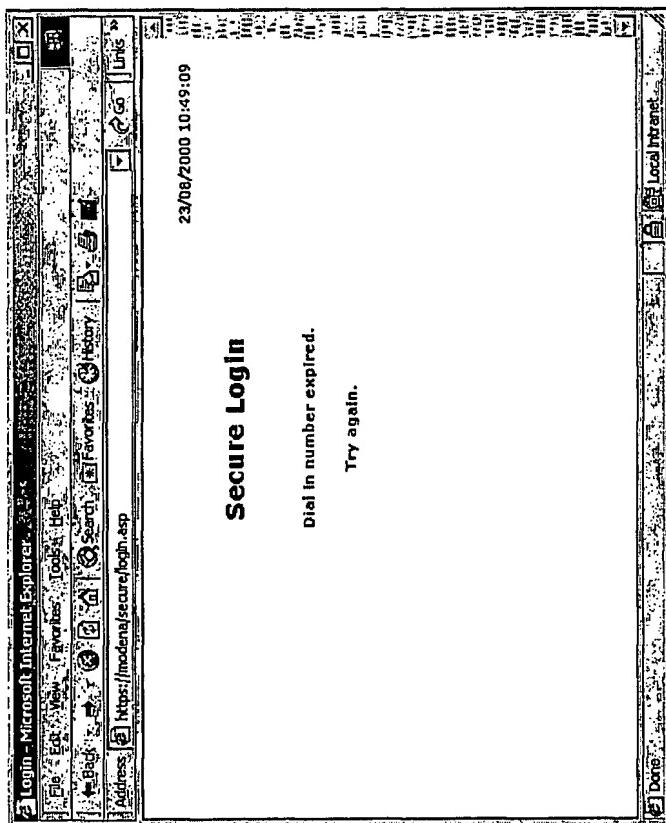


Fig 7

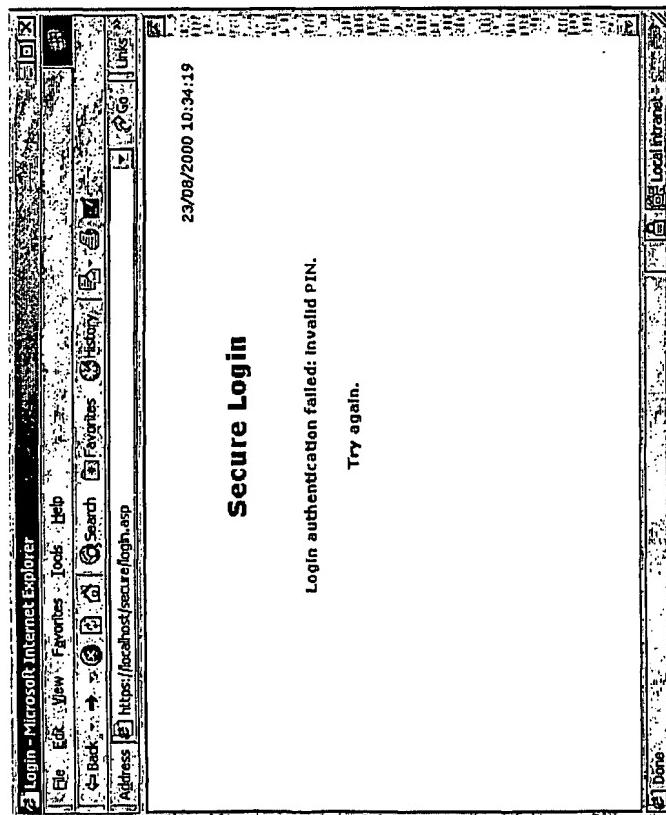


Fig 6

7/8

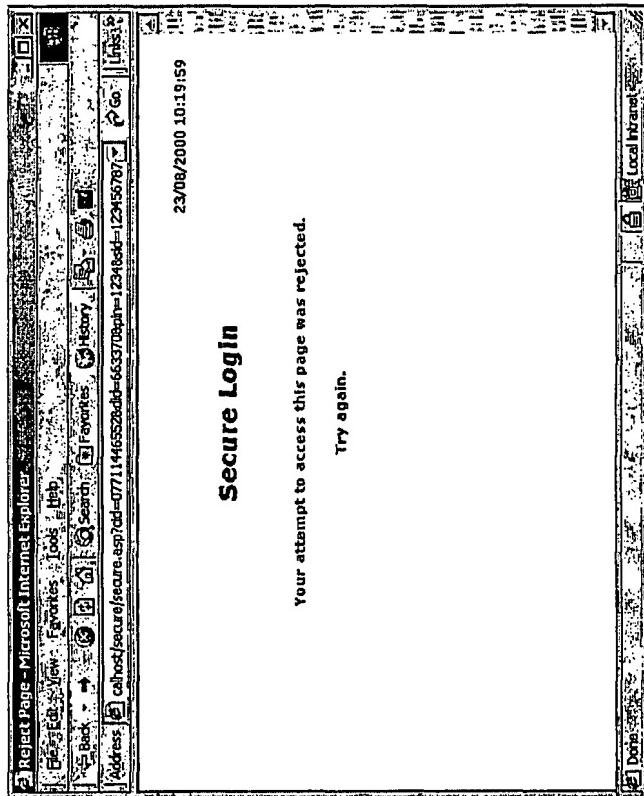


Fig 9

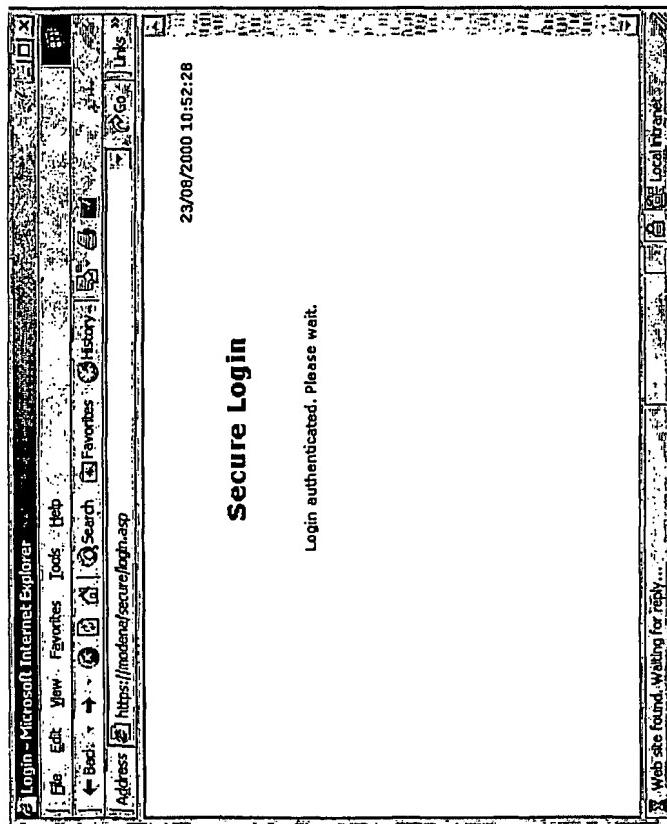


Fig 8

8/8

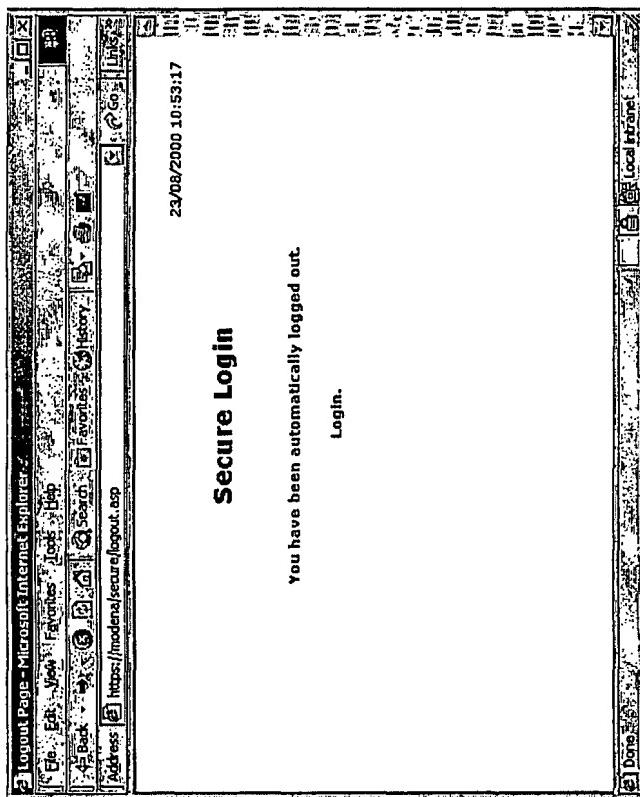


Fig 11

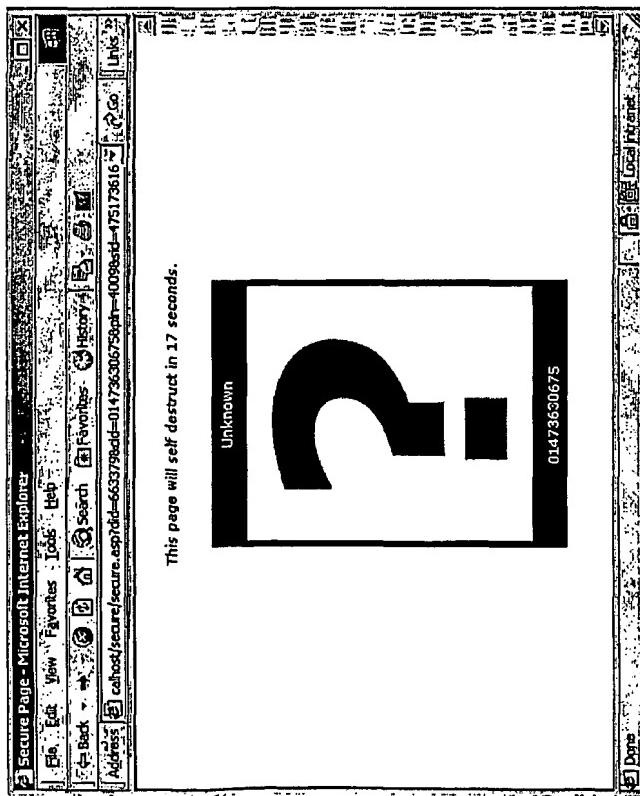


Fig 10